IN THE CLAIMS

1-33. (cancelled)

34. (currently amended) An information processing device operable within a node of a hierarchical network of nodes having a hierarchical tree structure, said information processing device comprising:

storage operable to store one or more node keys, each node key being unique to one node of the network, and a leaf key, the leaf key being unique to the information processing device and unique in relation to a leaf key held by any other node within the hierarchical network of nodes; and

an encryption processor operable to:

decrypt an encrypted renewal node key of a key block to obtain a renewal node key using at least one of the node key stored in the storage or a leaf key belonging to a lower layer of the hierarchical network and stored in the storage,

calculate a decryption key using the obtained renewal node key, ~~by decrypting a key block using at least one of the one or more node keys stored in the storage or the leaf key stored in the storage,~~

encrypt the decryption key using the leaf key of the information processing device,

store the encrypted decryption key in at least one of the storage or on a recording medium together with a generation number, the generation number representing renewal information for the decryption key, and

use the generation number to determine whether it is necessary to decrypt a key block corresponding to the generation number to obtain the decryption key.

35-47. (cancelled)

48. (currently amended) An information processing method, comprising:

storing one or more node keys and a leaf key in an information processing device of one node of a hierarchical

information processing device of one node of a hierarchical network of nodes having a hierarchical tree structure, each node key being unique to one node of the network, the leaf key being unique to the information processing device such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network;

decrypting a key block including an encrypted renewal node key, the renewal node key being encrypted using at least one of the stored node key for the node or a leaf key belonging to a lower layer of the hierarchical network, ~~using~~ at least one of the stored node key and the stored leaf key being used to decrypt the encrypted renewal node key to obtain a renewal node key;

using the obtained renewal node key to calculate~~calculating~~ a decryption key usable to decrypt encrypted data stored on at least one of the information processing device or on a recording medium;

encrypting the decryption key using the leaf key of the information processing device; and

storing the encrypted decryption key on at least one of the information processing device or on the recording medium together with a generation number representing renewal information for the decryption key;

using the stored generation number to determine whether the encrypted decryption key is stored on the at least one of the information processing device or on the recording medium; and

when it is determined that the encrypted decryption key is stored on the at least one of the information processing device or on the recording medium, using the leaf key to decrypt the encrypted decryption key to obtain the decryption key and using the decryption key to decrypt the encrypted data without having to decrypt the key block.

49-73. (cancelled)